

W → Strobe Talbott, below &
7.9 → yes
cm



Approved for Release 2005/04/12 : CIA-RDP88-01315R000400350010-2
CURRENT NEWS
SPECIAL EDITION

PA/STAFF
IF-06
DEPARTMENT OF THE AIR FORCE
UNITED STATES OF AMERICA

THIS PUBLICATION IS PREPARED BY THE AIR FORCE AS EXECUTIVE AGENT FOR THE DEPARTMENT OF DEFENSE TO BRING TO THE ATTENTION OF KEY DOD PERSONNEL NEWS ITEMS OF INTEREST TO THEM IN THEIR OFFICIAL CAPACITIES; IT IS NOT INTENDED TO SUBSTITUTE FOR NEWSPAPERS, PERIODICALS AND BROADCASTS AS A MEANS OF KEEPING INFORMED ABOUT THE NATURE, MEANING AND IMPACT OF NATIONAL AND INTERNATIONAL NEWS DEVELOPMENTS. USE OF THESE ARTICLES HERE, OF COURSE, DOES NOT REFLECT OFFICIAL ENDORSEMENT. FURTHER REPRODUCTION FOR PRIVATE USE OR GAIN IS SUBJECT TO THE ORIGINAL COPYRIGHT RESTRICTIONS.

6 DECEMBER 1979 No. 498

International Security
FALL 1979
Page 3
CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS HARVARD UNIVERSITY

ORIGI SALT

Scrambling and Spying in SALT II | *Strobe Talbott*

One of the most intractable issues in current arguments surrounding SALT II ratification concerns U.S. verification of the negotiated agreements. But the uncertainties about the technical and political problems of verification have hardly been confined to the domestic U.S. debate. The following article is based on the verification/telemetry controversies discussed in different parts of Strobe Talbott's forthcoming book, *Endgame: The Inside Story of SALT II* (Harper and Row). We believe that intra-governmental negotiations can best be shown by a focus on the specific topic of encryption. The analysis of how the United States dealt with the related problems of verification and telemetry shows the intra-governmental disputes and interaction of diplomacy and technology that characterize strategic arms negotiations in the nuclear age.

The article includes many quotations and references that cannot be footnoted. We find it understandable that these participants in SALT II feel constrained from personalizing their views. An article of such frankness and detail would not have resulted if all interviews had been for the record. Whatever the outcome of the dispute over SALT II, the process of protracted strategic arms negotiations between the superpowers will likely continue in some fashion, replete with the frustrations and conflicts presented below.

—The Editors

As they moved slowly toward an agreement on the definition of a new ICBM, the United States and the Soviet Union found themselves confronted with a related and extremely sensitive issue: the encryption of telemetry during the flight-testing of missiles. Telemetry is the electronic means by which a rocket, or a stage of a rocket, or a warhead sends back to earth data about its performance during a test flight. One way the United States could police Soviet compliance with SALT is to intercept and analyze Soviet telemetry. But the United States listens in on Soviet telemetry for purposes of espionage as well as arms control. It monitors Soviet tests to collect information that is valuable as military intelligence but irrelevant to the verification of agreements. The Soviets have never learned to live comfortably with the proficiency and what must seem to them like the near-omniscience of American surveillance. As

Strobe Talbott is Diplomatic Correspondent of Time magazine. This article is an excerpt from *Endgame* which will be published by Harper & Row in October 1979. Copyright © 1979 by Strobe Talbott. All rights reserved.

the most secretive and paranoid sectors of a secretive and paranoid society; the Soviet military and intelligence establishments have, by all indications, found American prying well-nigh intolerable, regardless of whether monitoring is carried out in the name of arms control. Therefore the Soviets have, from time to time, scrambled or otherwise put into code their missile telemetry in order to inhibit remote eavesdropping by the United States. It should be added that encryption also makes it harder for the Russians to read their own telemetry. The data is contained on lengthy computer printouts that look like a chaos of myriad broken lines on scores of channels, each line representing a fuel valve or a component of the guidance instrumentation as it switches on or off. Even when telemetry is transmitted in the clear, deciphering it requires the most painstaking analysis by the technicians running the test as well as those spying on it. Every time the Russians have used code, officials in the U.S. government, particularly those in the intelligence community, have tended to give a nervous jump and worry about the long-term implications for SALT.

How could the United States be confident that the Soviet Union is abiding by SALT if the Russians encrypt their telemetry? It was a question that sparked heated debate within the government, but U.S. officials have traditionally been reluctant to raise the issue at the negotiating table for a number of reasons. For one, the more the United States remonstrates the Soviets about their encryption practices, the more the Soviets will know about the American capability to intercept and decode their transmissions. And the more the Soviets know, the easier it will be for them to take countermeasures. To make encryption a topic of negotiation, in short, is to run the risk of "compromising intelligence sources and methods." Also, American officials knew that if they remonstrated to the Russians about encryption, the ensuing conversation might not be entirely one-sided. The United States, too, has used encryption and other methods of depriving foreign intelligence services of telemetric information about the testing of American systems, and the Pentagon has wanted to be able to do so in the future.

Said one member of the U.S. SALT delegation in Geneva, "Our side has never encrypted anything that is SALT-related." A senior Pentagon official put it this way: "Our record is as pure as the driven snow where ICBM tests and encryption are concerned. Both men were choosing their words very carefully. But the Defense Department, with the explicit approval of the Secretary of Defense in each case, has used encryption in testing some

shorter-range missiles and an anti-ballistic missile radar; on at least one occasion, the United States encrypted signals back to earth from a single-warhead ICBM, but the coded information concerned the performance of an ABM system "watching" the missile—not the performance of the missile itself. The United States has also transmitted telemetry at very low levels of power to highly directional antennas. Such a technique permits the use of a lighter-than-normal power pack aboard the top stage of the rocket. That means a lighter payload, which can be important in testing small ICBMs of the sort in which the United States specializes. But while the purpose of low-power telemetry transmission may simply be to save weight, its effect can be to make it more difficult for the other side to monitor the transmission. Thus it can be a form of "telemetry denial." Also, the United States has used capsules—like the black-box flight recorders aboard airliners—to retrieve information about the performance of ICBM components during re-entry into the atmosphere, when the extreme temperatures generated by friction make telemetric transmission impossible. Any comprehensive discussion of or ban on, encryption would probably have to extend to low levels of power and encapsulation too, since capsules are even more effective than codes if one side wishes to "black out" a test. Codes, after all, can be—and often are—broken. Capsules must be—and almost never are—captured.

Conflict in Geneva and Washington

Because of the extreme complexity and sensitivity of the issue, encryption was, for a long time, not only never discussed in Geneva—the very word was taboo.¹ Under instructions from Washington, Director of ACDA and chief negotiator Paul Warnke and his deputy Ralph Earle sought Soviet assent in the U.S. position that the SALT prohibition against "deliberate concealment measures which impede verification by national technical means" covered what Warnke and Earle referred to only as "methods of transmitting telemetric information." Alexander Shchukin, who was a specialist in radio wave theory and therefore the most knowledgeable Soviet

¹ Until July 1976, even the word "telemetry" had been taboo in the negotiations. Henry Kissinger, James Schlesinger and Donald Rumsfeld had all signed off on orders to the U.S. delegation in Geneva that telemetry was not to be mentioned in discussion of the ban on deliberate concealment measures. It was the Soviets who, for reasons that are still obscure, first introduced the word "telemetry" into the negotiations. The Carter Administration then allowed the negotiators to follow suit.

negotiator on the subject of telemetry, sometimes teased the Americans: "Why are you delivering your message in code—encrypted, as it were?" But the Soviets talked in code, too, and their message was quite different. They contended that the prohibition on "deliberate concealment measures which impede verification by national technical means" should not apply to "current test practices." Without uttering the taboo word, they were taking the position that telemetry used in missile tests is not relevant to SALT and that encryption of test telemetry should therefore be treated as an exemption to the ban against concealment measures.

Warnke and Earle argued that in testing, as in any other practice, the Soviets should be forbidden under SALT to do anything that "impeded" verification. Warnke once asked one of the U.S. interpreters if "impede" meant the same thing in Russian that it means in English. It means "to make more difficult," the interpreter replied. "There," said Warnke to Semyonov, the head of the Soviet delegation, "we are simply asking you to undertake not to do anything in your testing practices that would make verification more difficult." By September 1977, Semyonov had finally conceded that point as a general principle, although without explicit reference to encryption. Warnke and Earle felt that the issue had been laid to rest—without anyone's ever having uttered the word. The Soviets would be allowed to use encryption to protect genuine intelligence secrets, such as matters relating to the guidance system of a missile, while the United States would be free to raise before the Standing Consultative Commission in Geneva any case in which there was a suspicion that the Soviets might be using encryption to camouflage information necessary for verification, such as the number of warheads and throw-weight of the missile. Warnke, Earle and others were confident that the United States would know if encryption was being used to deprive American intelligence of information it needed for purposes of verification as opposed to espionage. The principal reason for their confidence was that the monitoring of telemetry is only one of a number of "national technical means" used to verify SALT, and there is considerable overlap—or "redundancy," as it is known—among those various means. Even if the Soviets successfully disguised a SALT-related feature of a missile test by encryption, that feature would likely show up on a radar screen or a satellite photograph or in some other piece of evidence available to the American monitors. Also, the memory banks of the computers used by U.S. intelligence had already accumulated masses of telemetric data from the Soviet ICBM testing program. If a channel of telemetry regularly used to

transmit SALT-related information in the past were suddenly scrambled or otherwise blacked out in a new test, the U.S. experts would be alerted to look even more closely at the evidence extracted by other national technical means, and, if their suspicions were sustained, to ask the American representatives on the Standing Consultative Commission to challenge the Soviets. Most American officials were quite satisfied with the way the Commission had worked throughout the life of SALT I. Each side had questioned suspicious or ambiguous activities of the other, and—with the notable exception of the environmental shelters covering ICBM silos at Malmstrom Air Force Base—the activity in question had been adequately explained, altered or halted. Warnke, Earle and like-minded officials back in Washington, including Secretary of State Vance, were certain that the consultative process could be extended to SALT II in a way that would guarantee American access to the Soviet telemetry necessary for verification of the new-types ban and the fractionation freeze.

But that sanguine view was not unanimous within the Carter Administration, and in late 1977 the Administration changed the signals it was sending to Geneva. CIA officials said they were increasingly concerned about their ability to verify a SALT II agreement that was explicit and restrictive in its definition of new types of missiles but circumspect and therefore seemingly permissive in the way it addressed the problem of encryption. Stansfield Turner, the director of Central Intelligence, and Robert Bowie, his principal deputy for National Intelligence Estimates, argued that they would not only have difficulty verifying the prospective treaty, they would have difficulty defending its ratification before the Senate, if encryption was dealt with obliquely. Ratification was increasingly on the minds of the policymakers, and encryption went to the heart of the American obsession with verification. Ohio Senator John Glenn staked out encryption as his own issue. As a congressional adviser to the SALT delegation, Glenn had visited Geneva in August 1977 and stressed to Semyonov and Shchukin that his vote for or against ratification would depend largely on how encryption was handled in the treaty. He also told the American negotiators that by avoiding mention of encryption, they were "obfuscating" the issue.

Over several months, the CIA changed its position a number of times. At one point, Turner and Bowie argued for an across-the-board ban on encryption—an idea that John Glenn and Paul Nitze advocated too. President Carter at one point said he could support an outright ban. But Cyrus Vance and Paul Warnke took the view that there was no way the Soviets would ever,

in their technology before SALT II came into force, but they were probably also seeking to lay down a base line of what they considered permissible encryption and at the same time probing the American ability to monitor such tests. "They were smoking us out," said one U.S. intelligence official. "They wanted to see how quickly we responded, how much we revealed about knowledge of their transmissions, and how upset we were."

Stansfield Turner was very upset indeed. At a series of meetings, he took a harder line than ever on encryption. Turner and the CIA, after all, were in the business of monitoring Soviet military activity, and no one could dispute that encryption made their task more difficult. It was a case in point of the Washington adage, "Where you stand is where you sit." Turner sat in a job that required him both to verify SALT and to defend its verifiability to the Senate, so it was not surprising that he stood for a ban on encryption.

On few issues in SALT have the national interests and negotiating strategies of the two sides been so clearly at odds as they were on encryption. The United States pursued a comprehensive definition of new types that would genuinely curtail the modernization of Soviet missiles. The more meaningful the definition, the more it required explicit restrictions on encryption in order to be verified. The Soviets, for their part, sought to minimize the number of parameters in the new-types definition in order to maintain the freedom to upgrade their missiles but also, some analysts have speculated, to maintain maximum freedom to encrypt. The encryption issue had brought the CIA into the center of SALT policy-making in Washington. No doubt the issue had a mirror-image effect in Moscow. The KGB and the other Soviet intelligence services almost certainly bridled at what they considered an American attempt to use an arms control agreement to pry deeper into Soviet military secrets. This complicating factor was only hinted at in Geneva, where Semyonov and his colleagues began making statements like, "National technical means does not legitimate overhead espionage." As one American official put it, "All of a sudden, the Soviets started taking the lofty and offended position that gentlemen do not read each other's telemetry." The U.S. negotiators persisted in arguing that for the new-types rule to be enforceable—indeed, for the overall prohibition against deliberate concealment to be meaningful—there had to be a "common understanding" which explicitly identified encryption as a testing practice that would be forbidden if it impeded verification. The pursuit of treaty language on that point was made more difficult by the fact that on this critical and delicate issue, the intelligence services of the two sides now had their backs up. They were

taking a more active and mistrustful part in the home-office supervision of the Geneva negotiators than ever before.

A Proposal of Marriage

At the December 1978 meeting in Geneva between Vance and Gromyko, the two diplomats also spent considerable time on the thorny issue of telemetry encryption. After the Moscow meeting in October, at which Gromyko had rejected the American contention that SALT must explicitly ban any encryption which hindered the monitoring of compliance, the problem was remanded to the delegations in Geneva. But it was clearly a problem of such exquisite complexity and sensitivity that it could only be resolved at what the negotiators called "the political level"—between Vance and Gromyko themselves. They alone would have to agree on the wording of a "common understanding" in the Joint Draft Text that addressed the question of encryption. The American-preferred provision would have stressed what was forbidden—i.e., encryption "whenever it impeded" verification. Gromyko brought with him to Geneva, and gave to Vance on the first day of their talks, Soviet-preferred language that would have stressed what was permitted—i.e., encryption that did *not* impede verification. Vance emerged from the session hopeful. While the emphasis was different, the Soviet position was not incompatible with the American one. Most importantly, the Soviets seemed implicitly to be accepting a critical aspect of the American position: the *only* criterion for determining the permissibility or impermissibility of encryption should be whether or not the encryption in question impeded verification; there should be no burden on the United States to establish that a particular instance of Soviet encryption was deliberately intended to impede verification. The U.S. side wanted to avoid cases in the Standing Consultative Commission in which the American representatives would challenge the use of code and their Soviet counterparts could defend the practice by responding that the code was intended to protect legitimate military secrets, not to thwart American monitoring of SALT. According to the American formulation of the limited encryption ban, which the Soviets now seemed tacitly to accept, the intent of encryption was irrelevant to its permissibility; only its effect mattered. If its effect was to impede, then it would be forbidden, regardless of intent. That did not solve the potential problem of how to establish in the Standing Consultative Commission that a given use of code had impeded verification without at the same time telling

naissance drones and multiple-warhead cruise missiles, as well as a handful of other details. These, it was believed, could be left to the permanent delegations to dispose of while the Secretary of State and the Foreign Minister announced a mid-January summit at which Carter and Brezhnev would sign SALT II. General Seignious, as a member of the U.S. delegation, told Vance that he had found Gromyko far more flexible and agreeable than veterans of past encounters with the foreign minister had led him to expect. Seignious and Paul Warnke, who was now serving the administration as a part-time consultant on SALT, were sufficiently confident that the next morning's meeting would be *pro forma* and upbeat that they decided to miss it and to catch an early flight back to the United States so they would have some extra time with their families over Christmas weekend. Vance's chief press spokesman, Hodding Carter, cautioned newsmen that there was still no final agreement, but in reflecting the mood of the delegation encouraged the press to expect one the next day. "We are close to the end of the road," he said, echoing a line Vance himself was using to characterize the progress he felt had been made.

The wire services transmitted dispatches from Geneva suggesting that SALT was at hand. As soon as these stories reached the White House teletype machines, they were flashed to Air Force One, which was en route to Georgia. The President was going home to Plains for Christmas. Hamilton Jordan and Jody Powell were with him. Before leaving Washington, Jordan and Powell, along with Gerald Rofshoon, the White House media adviser, and Frank Moore, chief of congressional liaison, had held a series of meetings to prepare briefings on the agreement for the press and the Congress in the event that Vance and Gromyko were able to announce a date for the summit after their final session Saturday. The extremely positive wire service stories from Geneva suggested that an announcement was indeed imminent, yet the presidential party had still heard nothing directly from Vance.

Vance is Overruled

That Friday in the early evening, when Vance's reporting cable finally arrived, Zbigniew Brzezinski convened a meeting in his office in the corner of the White House West Wing. In addition to Brzezinski and his deputy David Aaron, were Harold Brown, Stansfield Turner, Warren Christopher, the deputy secretary of state, and Spurgeon Keeny, the deputy director of ACDA. It was supposed to be a short session. Brzezinski and Aaron were

due at the British ambassador's for a Christmas party. Their wives were waiting for them outside the office. But the meeting continued until nearly 11 p.m. It turned out to be long and contentious primarily because of the way Vance proposed to deal with the encryption issue. In his cable from Geneva, the Secretary of State explained that he and Gromyko had worked out language explicitly banning encryption "whenever it impedes" verification while explicitly permitting it when it does not impede verification. Stansfield Turner was already unhappy with the administration's decision not to seek an across-the-board ban on encryption. He felt the limited ban on which the United States had settled was a half-measure at best. For example, he objected to the notion that the SALT II document would go so far as to stipulate, in black and white, that encryption was allowed. In view of what he felt was the noncommittal nature of Gromyko's response to Vance's point about the July 29 test, Turner argued that the Soviets would have far too much leeway to decide for themselves when encryption impeded verification and when it did not; indeed, the Russians might well take the position that in actual practice, telemetry was never really necessary to verification and its encryption was therefore never really impermissible. After a lengthy, sometimes heated discussion, Turner said he could live with the common understanding on encryption that Vance and Gromyko had worked out if Vance stated the American objection to the July 29 test more bluntly and if Gromyko responded more satisfactorily. The Director of Central Intelligence proposed that at the next day's meeting in Geneva, Vance should raise the matter of the July 29 test again, this time seeking Gromyko's "concrete affirmation" that a repetition of such a test would be illegal under SALT II. Warren Christopher, referring to his own experience as a lawyer, warned against using the July 29 test as a benchmark for the legality of encryption; all the Soviets would have to do would be to encrypt one less channel than they had encrypted on July 29, still scrambling many others, and they could then claim they were staying within the bounds on which the Americans had insisted. "Whenever I've cited a specific example in pursuit of a general principle," said Christopher, "I've always regretted it later on." David Aaron agreed. He once remarked that no less a SALT personage than Paul Nitze, during his term as a negotiator in Geneva, had laid down a stern warning: "Never try to establish principles by citing examples. Otherwise the examples will come back and bite you later on." Roger Molander, a member of the National Security Council staff, who was consulted during the Friday night meeting, pointed out that if the United

to apply retroactively a provision of a treaty that was not yet concluded, much less in force. It seemed an attempt to get the Russians in effect to confess that they had done something wrong—that they had sinned against the spirit of SALT. Vance could tell that by carrying out his unwelcome new instructions, he had—just as he had feared—aroused Soviet hypersensitivity.

Conclusion: The Brezhnev-Carter Correspondence

On what had already become by January 1979 one of the thorniest of all the final sticking points—encryption of telemetry—neither side was satisfied with the negotiating record as it then stood. Vance and Gromyko had struck a bargain in Geneva just before Christmas to include in the treaty a common understanding that banned encryption when it impeded verification and permitted it when it did not. Vance had been pleased with that formulation because it meant the United States would have grounds for protesting any encryption that constituted an impediment, regardless of whether the Soviets were deliberately trying to impede verification or, as they would surely claim, merely trying to protect legitimate military secrets. However, Stansfield Turner and to a lesser extent Harold Brown and Zbigniew Brzezinski had not been content with the common understanding all by itself. They felt it left the Soviets too much latitude to argue that while hypothetically some encryption might be impermissible, in actual practice neither of those conditions had ever arisen, nor was likely to arise. Therefore Turner, Brown and Brzezinski wanted the common understanding in the treaty reinforced by a formal exchange in the negotiating record. In this exchange the Russians would acknowledge that Soviet encryption *as already practiced* had met the criterion of impermissibility stipulated by the common understanding and that a repetition of that practice would be a violation.

In January, Ralph Earle went through the same exercise with Victor Karpov in Geneva. Earle cited not only the July 29 test but the similar December 21 test as well. "If you disagree" with the American position, said Earle, concluding the ritual, "tell me now." Karpov, like Gromyko before, was being given a chance to speak now or forever hold his peace. He held his peace, but not forever. One trouble with the diplomatic device of non-contradiction is that an understanding arrived at by the silence of one party is easily undone; all that party has to do is break silence. That is exactly what Karpov did. On February 14 he came back to Earle and told him he was "under instructions from my government" to state that the previously agreed com-

mon understanding on encryption was adequate to cover any case that might arise and that there was "no need for further interpretation." It was the Soviets' way of saying that they neither accepted nor rejected the American position—and that they did not want to hear the subject raised again.

Back in Washington, where Karpov's statement was known in some offices as "the Kremlin's Valentine," the interagency squabble over how to handle the encryption issue started all over again. At the State Department and ACDA there was little dismay, and even less surprise, that the Soviets were still refusing to admit that they had done anything wrong on July 29 and December 21. One official, who had opposed the attempt to get Soviet "non-contradiction" all along, commented sardonically, "the whole episode was just another example of how you can always find trouble if you're imaginative and persistent enough in the way you look for it. If you keep pressing the Russians for greater and greater specificity, sooner or later they're going to balk and you're going to end up jeopardizing a very useful general agreement. Frankly, I don't blame the Russians one bit for throwing our interpretation right back in our faces."

But even those who felt a degree of sympathy with the Soviet position recognized that Karpov's latest statement raised a serious political problem. In its upcoming effort to win the support of John Glenn and other senators, the Administration had been counting on demonstrating that it had extracted from the Soviets what amounted to a promise never again to encrypt as much telemetry as they had on July 29 and December 21, and specifically not to encrypt the telemetry from the reentry vehicles. Karpov's statement had the predictable effect of throwing Stansfield Turner into a relapse of agitation on the issue. Having never really made his peace with the common understanding and still regarding the noncontradiction device as a half-measure at best, he now felt justified in trying again to get an across-the-board prohibition of encryption. At a Special Coordination Committee of the NSC meeting on March 5, Turner suggested a number of options for handling the problem now that Karpov had reopened the issue, and the option obviously closest to Turner's heart was to "ban all telemetry denial, including encryption," in the testing of any missile covered by SALT.

The other members of the SCC, notably Brown and Brzezinski, shared Turner's concern but did not believe there was any hope of getting the Soviets to accept an outright ban on encryption. As one official involved in the deliberations recalled, "The essence of the problem was that under the harshest interpretation, the Soviets might be leaving open the implication